An Alternative Approach to Implementing New Technology

November 2011

Here's an interesting look into the inner workings of international cyber criminals by virtue of covertly recorded conversation snippets. The characteristics of similar processes in Western governments, particularly here in the U.S., are well known because they are described in detail in the media. Our processes exist to provide accountability, budget constraint, quality assurance and fair competition. The bad guys have a slightly different take on how to go about things.

Bad Guy Procurement Process: Sell some drugs, stolen technology, body parts or slaves and buy 500 mobile communication devices to give to our Research and Development Group. Actually, try stealing them first. Do this by tomorrow, yes?

Bad Guy R&D Incentive Package: Find a way to hack into this mobile device and I will give you a million Euros. Fail to do so and I will have all of your extremities cut off with a dull, rusty hacksaw. I'll let you know when your time is up. Good luck!

Bad Guy Program Approval Process: Mr. Big wants this done. Yes, the Mr. Big who had all of his inner council tortured because the frosting his birthday cake wasn't sweet enough. So, by tomorrow then? Good! Thanks for your support of our initiative.

Bad Guy Market Research: I just read the American military is thinking about using Mobile Electronic Devices. Tell our 500,000 expert hackers around the world to start focusing on this. (two hours later). So the Army is going to be starting a pilot program on smart phones. When? Next Year? A general just suggested this in an email to the Deputy Secretary a half hour ago? How come I didn't hear about it sooner?!?!? Still, it's nice to be ahead of the curve.

Bad Guy's Resource Allocation Decision Process: You need a million computers to launch the cyber attack? These computers will be destroyed or abandoned afterwards? Even if the attack doesn't work it will cause a panic attack in most military risk mitigation groups requiring additional outlays of time and resources to build a defense? Sounds like a winner. Is a million enough? We've got warehouses full of them around the world.

Bad Guy Internal Conflict Resolution: I heard the four of you differ on who should get the credit for the development of the new Super Worm and this is delaying our releasing it to military and business networks around the world. Hmmm. You actually tweeted about this? Really? <BANG!> You. I just don't agree with you. <BANG!> Now, both of you have good arguments. I can't seem to decide which…..<BANG!> Ah, I see you've worked it out amongst yourselves. Good. Let's get back to work shall we? I like short meetings.

What we can learn from these small but enlightening bits of intel is that the bad guys are always going to be able to throw significant resources, people and money at defeating our security programs and processes. This doesn't mean that we can't do it. What it does mean is that every time someone circumvents established policies, procedures and best practices, there's an excellent chance that the bad guys are ready to exploit that vulnerability in an instant. Think about that as you develop you own apps or download apps from unapproved sources. The rules are there for a reason. Technology can build very strong doors, but it is the individual that turns the key.